on the receiving side is able to know the third conversion constant that corresponds to the pattern-conversion constant contained in the received signal, and is able to decode the transmission data from the first signal and second signal.

By doing this, even though the first signal and second signal may be leaked during transmission, it is not possible for a third party who does not know the third conversion constant corresponding to the pattern-conversion constant to decode the transmission data, and thus it is possible to maintain confidentiality.

Also, in the case of a fraudulent transmission, the relationship between the pattern-conversion constant contained in the second signal of the fraudulent transmission, and the third conversion constant used in encrypting the transmission data does not match the relationship between the proper pattern-conversion constant and the third conversion constant, so the decoded data that is decoded from both signals is not decoded as meaningful data, and thus it is possible to easily determine that the transmission is fraudulent.

As described above, together with making it possible to prevent trouble due to fraudulent transmission by performing personal authentication of the sender on the receiving side even when a third party posing as the original sender sends data, this invention also makes it possible to provide a data-transmission system, data-transmission method and data-transmission apparatus for transmitting highly confidential data.

WHAT IS CLAIMED IS:

1. A data-transmission system that sends transmission data, which has been encrypted by using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises: a conversion-constant selection means of selecting said first conversion constant, said second

conversion constant and said third conversion constant; an encryption means of using said second conversion constant, or said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant, or said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value; a first-signal-generation means of generating a first signal that contains said first substitute value and said first conversion constant; a memory means of storing a pattern-conversion constant that corresponds to said third conversion constant; a second-signal-generation means of generating a second signal that contains said second substitute value, said second conversion constant and said pattern-conversion constant; and a transmission means of sending said first signal to said apparatus on the receiving side and said second signal to a relay apparatus;

said relay apparatus comprises: a memory means of storing a third conversion constant that corresponds to said pattern-conversion constant; a signal-generation unit that receives said second signal, and converts said pattern-conversion constant contained in said second signal to said third conversion constant to generate a second' signal; and a transmission means of sending said second' signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises: a reading means of receiving said first signal from said apparatus on the sending side and said second' signal from said relay apparatus, and reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said third conversion constant from said second' signal; a decoding means of using said conversion constants that were used in encrypting said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and an authentication means of authenticating said first signal and said second' signal from said first

decoded data and said second decoded data.

2. A data-transmission system that sends transmission data, which has been encrypted by two conversion constants from among a first conversion constant, second conversion constant, third conversion constant, and fourth conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises: a conversion-constant-selection means of selecting said first conversion constant, said second conversion constant, said third conversion constant and said fourth conversion constant; an encryption means of using said second conversion constant and said fourth conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value; a memory means of storing pattern-conversion constants that correspond to said third conversion constant and said fourth conversion constant; a first-signal-generation means of generating a first signal that contains pattern-conversion constants that correspond to said first substitute value, said first conversion constant, and said third conversion constant or said fourth conversion constant; a second-signal-generation means of generating a second signal that contains pattern-conversion constants that correspond to said second substitute value, said second conversion constant, and said third conversion constant or said fourth conversion constant that is not contained in said first signal; and a transmission means of sending said first signal to a first relay apparatus and sending said second signal to a second relay apparatus;

said first relay apparatus comprises: a memory means of storing a third conversion constant or fourth conversion constant that corresponds to said pattern-conversion constant; a signal-generation means of receiving said first signal and converting the pattern-conversion constant contained in that signal to said third conversion constant or said fourth conversion

constant to generate a first' signal; and a transmission means of sending said first' signal to said apparatus on the receiving side;

said second relay apparatus comprises: a memory means of storing a third conversion constant or fourth conversion constant that corresponds to said pattern-conversion constant, a signal-generation means of receiving said second signal and converting said pattern-conversion constant contained in that signal to said third conversion constant or said fourth conversion constant to generate a second' signal; and a transmission means of sending said second' signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises: a reading means of receiving said first' signal and said second' signal and reading said first substitute value , said first conversion constant and said third conversion constant or said fourth conversion constant from said first' signal, and reading said second substitute value, said second conversion constant and said third conversion constant or said fourth conversion constant from said second' signal; a decoding means of using the conversion constants that were used for encrypting said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and an authentication means of performing authentication of said first' signal and said second' signal from said first decoded data and said second decoded data.

3. A data-transmission system that sends transmission data, which has been encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises: a conversion-constant-selection means of selecting said first conversion constant, said second conversion constant and said third conversion

constant; an encryption means of using said second conversion constant, or said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant, or said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value; a first-signal-generation means of generating a first signal that contains said first substitute value and said first conversion constant; a memory means of storing a pattern-conversion constant that corresponds to said third conversion constant; a second-signal-generation means of generating a second signal that contains said second substitute value, said second conversion constant and said pattern-conversion constant; and a transmission means of sending said first signal and said second signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises: a reading means of receiving said first signal and said second signal, and reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said pattern-conversion constant from said second signal; a memory means of storing a third conversion constant that corresponds to said pattern-conversion constant; a reading means of reading said third conversion constant from said read pattern-conversion constant; a decoding means of using the conversion constants that were used to encrypt said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and an authentication means of authenticating said first signal and said second signal from said first decoded data and second decoded data.

4. The data-transmission system of claim 1 or claim 3 wherein said encryption means uses said second conversion constant and third conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant and said third conversion constant

to encrypt said transmission data to a second substitute value.

5. The data-transmission system of claim 1 or claim 3 wherein said encryption means uses said second conversion to encrypt said transmission data to a first substitute value, and uses said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value.

6. The data-transmission system of claim 1 or claim 3 wherein said encryption means uses said second conversion constant and third conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant to encrypt said transmission data to a second substitute value.

7. The data-transmission system of any one of the claims 1 to 3 wherein said apparatus on the receiving side further comprises a drive-signal-transmission means of sending a drive signal for driving an external-drive apparatus based on said first decoded data and second decoded data.

8. The data-transmission system of any one of the claims 1 to 3 wherein said authentication means performs said authentication when said first decoded data and said second decoded data match.

9. The data-transmission system of claim 1 or claim 2 wherein said apparatus on the sending side, said relay apparatus and said apparatus on the receiving side are connected to a communications network that includes the Internet.

10. The data-transmission system of claim 3 wherein said apparatus on the sending side and said apparatus on the receiving side send or receive signals by an infrared signal method, wireless signal method, optical

communication method or wired communication method.

11. A data-transmission method that sends transmission data, which has been encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises:

a step of selecting said first conversion constant, said second conversion constant and said third conversion constant;

an encryption step of using said second conversion constant, or said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant, or said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value;

a first-signal-generation step of generating a first signal that contains said first substitute value and said first conversion constant;

a second-signal-generation step of generating a second signal that contains said second substitute value, said second conversion constant and a pattern-conversion constant that corresponds to said third conversion constant; and

a first transmission step of sending said first signal to said apparatus on the receiving side and said second signal to a relay apparatus;

said relay apparatus comprises:

a conversion step of receiving said second signal, and converting the pattern-conversion constant contained in said second signal to said corresponding third conversion constant to generate a second' signal; and

a second transmission step of sending said second' signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises:

a reading step of receiving said first signal from said apparatus on

the sending side and said second' signal from said relay apparatus, and reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said third conversion constant from said second' signal;

a decoding step of using the conversion constants that were used in encrypting said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and

an authentication step of authenticating said first signal and said second' signal from said first decoded data and said second decoded data.

12. A data-transmission method that sends transmission data, which has been encrypted using two conversion constants from among a first conversion constant, second conversion constant, third conversion constant and fourth conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises:

a selection step of selecting said first conversion constant, said second conversion constant, said third conversion constant and said fourth conversion constant;

an encryption step of using said second conversion constant and said fourth conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value;

a first-signal-generation step of generating a first signal that contains said first substitute value, said first conversion constant, and pattern-conversion constant that corresponds to said third conversion constant or said fourth conversion constant;

a second-signal-generation step of generating a second signal that contains said second substitute value, said second conversion constant,

and pattern-conversion constant that corresponds to said third conversion constant or said fourth conversion constant that is not contained in said first signal; and

a first transmission step of sending said first signal to a first relay apparatus, and sending said second signal to a second relay apparatus;

said first relay apparatus and said second relay apparatus comprise:

a conversion step of receiving said first signal or said second signal and converting said pattern-conversion constant contained in that signal to corresponding said third conversion constant or said fourth conversion constant to generate a first' signal or second' signal; and

a second transmission step of sending said first' signal or said second' signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises:

a reading step of receiving said first' signal and said second' signal, and reading said first substitute value, said first conversion constant and said third conversion constant or said fourth conversion constant from said first' signal, and reading said second substitute value, said second conversion constant and said third or said fourth conversion constant from said second' signal;

a decoding step of using the conversion constants that were used in encrypting said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and

an authentication step of authenticating said first' signal and said second' signal from said first decoded data and said second decoded data.

13. A data-transmission method that sends transmission data, which has been encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, from an apparatus on the sending side to an apparatus on the receiving side, wherein

said apparatus on the sending side comprises:

a step of selecting said first conversion constant, said second conversion constant and said third conversion constant;

an encryption step of using said second conversion constant or said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and using said first conversion constant or said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value;

a first-signal-generation step of generating a first signal that contains said first substitute value and said first conversion constant;

a second-signal-generation step of generating a second signal that contains said second substitute value, said second conversion constant and a pattern-conversion constant that corresponds to said third conversion constant; and

a transmission step of sending said first signal and said second signal to said apparatus on the receiving side; and

said apparatus on the receiving side comprises:

a reading step of receiving said first signal and said second signal and reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said pattern-conversion constant from said second signal;

a conversion-constant-acquisition step of acquiring said third conversion constant that corresponds to said read pattern-conversion constant;

a decoding step of using the conversion constants that were used to encrypt said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and

an authentication step of authenticating said first signal and said second signal from said first decoded data and said second decoded data.

14. The data-transmission method of claim 11 or claim 13 wherein in said encryption step said second conversion and said third conversion constant are used to encrypt said transmission data to said first substitute value, and said first conversion constant and said third conversion constant are used to encrypt said transmission data to said second substitute value.

15. The data-transmission method of claim 11 or claim 13 wherein in said encryption step, said second conversion constant is used to encrypt said transmission data to said first substitute value, and said first conversion constant and said third conversion constant are used to encrypt said transmission data to said second substitute value.

16. The data-transmission method of claim 11 or claim 13 wherein in said encryption step, said second conversion constant and said third conversion constant are used to encrypt said transmission data to said first substitute value, and said first conversion constant is used to encrypt said transmission data to said second substitute value.

17. The data-transmission method of any one of the claims 11 to 13 wherein after said authentication step, said apparatus on the receiving side further comprises a drive-signal-transmission step of sending a drive signal for driving an external-drive apparatus based said first decoded data or said second decoded data.

18. The data-transmission method of any one of the claims 11 to 13 wherein in said authentication step, authentication is performed when said first decoded data matches said second decoded data.

19. An apparatus that sends data that has been encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant comprising:

a memory unit that stores pattern-conversion constants that corresponds to said conversion constants;

a control unit, which performs a conversion-constant-selection process of selecting said first conversion constant, said second conversion constant and said third conversion constant, an encryption process of using said second conversion constant, or said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant, or said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value, a first-signal-generation process of generating a first signal that contains said first substitute value and said first conversion constant, a second-signal-generation process of generating a second signal that contains said second substitute value, said second conversion constant and said pattern-conversion constant that corresponds to said third conversion constant, and a transmission process of sending the first signal and second signal; and

a transmission unit that sends said first signal and said second signal to the outside.

20. The apparatus of claim 19 wherein said control unit uses said second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value.

21. The apparatus of claim 19 wherein said control unit uses said second conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value.

22. The apparatus of claim 19 wherein said control unit uses said

second conversion constant and said third conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant to encrypt said transmission data to a second substitute value.

23. An apparatus that sends data that has been encrypted using two conversion constants from among a first conversion constant, second conversion constant, third conversion constant and fourth conversion constant, and comprising:

a memory unit that stores pattern-conversion constants that correspond to the conversion constants;

a control unit, which performs a conversion-constant-selection process of selecting said first conversion constant, said second conversion constant, said third conversion constant and said fourth conversion constant, an encryption process of using said second conversion constant and said fourth conversion constant to encrypt said transmission data to a first substitute value, and uses said first conversion constant and said third conversion constant to encrypt said transmission data to a second substitute value, a first-signal-generation process of generating a first signal that contains said first substitute value, said first conversion constant and pattern-conversion constant that corresponds to said third conversion constant or said fourth conversion constant, and a second-signal-generation process of generating a second signal that contains said second substitute value, said second conversion constant and pattern-conversion constant that corresponds to said third conversion constant or said fourth conversion constant that is not contained in said first signal; and

a transmission unit that sends said first signal and said second signal to the outside.

24. An apparatus that transfers a signal that contains pattern-conversion constants corresponding to the conversion constants

that are used in encrypting the transmission data, and comprising:

a memory unit that stores pattern-conversion constants that corresponds to said conversion constants;

a transmission/reception unit that sends and receives said signal; and

a control unit that performs

a signal-generation process of converting said pattern-conversion constants contained in said received signal to said conversion constants to convert said signal, and

a process of transferring said converted signal.

25. An apparatus that receives a first signal and second' signal that contain transmission data that was encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, and decodes the transmission data and comprises:

a receiving unit that receives said first signal and said second' signal, wherein

said first signal contains a first substitute value, which is said transmission data that has been encrypted using said second conversion constant, or said second conversion constant and said third conversion constant, and said first conversion constant, and

said second' signal contains, a second substitute value, which is said transmission data that has been encrypted using said first conversion constant, or said first conversion constant and said third conversion constant, said second conversion constant and said third conversion constant; and

a control unit that performs a process of reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said third conversion constant from said second' signal; a decoding process of using the conversion constants that were used for encrypting said first

substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and an authentication process of authenticating said first signal and said second' signal from said first decoded data and said second decoded data.

26. An apparatus that receives a first' signal and a second' signal, which contain transmission data that has been encrypted using two conversion constants from among a first conversion constant, second conversion constant, third conversion constant and fourth conversion constant, and decodes the transmission data, and comprising:

a reception unit that receives said first' signal and said second' signal wherein

said first signal' contains a first substitute value, which is said transmission data that has been encrypted using said second conversion constant and said fourth conversion constant, said first conversion constant and said third conversion constant or said fourth conversion constant, and

said second' signal contains a second substitute value, which is said transmission data that has been encrypted using said first conversion constant and said third conversion constant, said second conversion constant and said third conversion constant or said fourth conversion constant that is not contained in said first' signal; and

a control unit that performs: a reading process of reading said first substitute value, said first conversion constant and said third conversion constant or said fourth conversion constant from received said first' signal, and reading said second substitute value, said second conversion constant and said third conversion constant or said fourth conversion constant from the received said second' signal; a decoding process of using the conversion constants that were used to encrypt said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data,

respectively; and an authentication process of authenticating said first' signal and said second' signal from said first decoded data and said second decoded data.

27. An apparatus that receives a first signal and a second signal that contains transmission data that has been encrypted using at least one conversion constant from among a first conversion constant, second conversion constant and third conversion constant, and decodes that transmission data, and comprising:

a memory unit that stores pattern-conversion constants that correspond to said conversion constants;

a reception unit that receives said first signal and said second signal, wherein

said first signal contains a first substitute value that was encrypted using said second conversion constant or said second conversion constant and said third conversion constant, and the first conversion constant, and

said second signal contains a second substitute value that was encrypted using said first conversion constant or said first conversion constant and said third conversion constant, said second conversion constant, and a pattern-conversion constant that corresponds to said third conversion constant; and

a control unit that performs: a reading process of reading said first substitute value and said first conversion constant from said first signal, and reading said second substitute value, said second conversion constant and said pattern-conversion constant from said second signal; an acquisition process of acquiring said third conversion constant from said read pattern-conversion constant; a decoding process of using the conversion constants that were used to encrypt said first substitute value and said second substitute value to decode said first substitute value and said second substitute value to first decoded data and second decoded data, respectively; and an authentication process of authenticating said first signal and said second signal from said first decoded data and said second